19. Active Directory - Enumeration

🧠 Active Directory Enumeration

🚨 Why is AD Enumeration Important?

🔐 For Administrators (Defensive Perspective):

- **Audit and secure** the environment.
- Detect **misconfigurations** and **over-permissioned accounts**.
- Identify **stale/unused objects** (users, machines).
- Monitor for **anomalies and early indicators** of attack.

💥 For Attackers (Offensive Perspective):

- **Reconnaissance**: Understand AD structure and targets.
- **Privilege escalation**: Identify privileged accounts and misconfigurations.
- **Lateral movement**: Map trust relationships and connected machines.
- **Persistence**: Find overlooked backdoors (e.g., shadow admin rights).

🛠️ Tools & Methods for AD Enumeration

Category	Examples & Techniques
Windows Commands	`net user`, `net group`, `dsquery`, `nltest`, `whoami`
PowerShell Cmdlets	`Get-ADUser`, `Get-ADGroupMember`, `Get-ADComputer`, `Get-GPO`
LDAP Queries	Query directory data using filters like `(&(objectClass=user))`
Third-Party Tools	BloodHound, SharpHound, ADRecon, LDAPSearch, CrackMapExec
Scripting	Custom PowerShell or Python scripts using `ldap3`, `Impacket`

🔍 What Can Be Enumerated?

Object	Purpose
Users	Detect high-privileged accounts, stale or misconfigured users
Groups	Identify admin or privileged groups (e.g., `Domain Admins`)
Computers	Spot outdated machines or weak naming conventions
Domain Controllers	Find out where authentication takes place

Object	Purpose
Trusts	Identify inter-domain/forest relationships exploitable for lateral movement
Group Policy Objects (GPOs)	Audit security policies (e.g., password policies, scripts)
ACLs/Permissions	Look for misconfigured delegations or excessive rights (e.g., DACLs on OUs)

📊 Interpreting Enumeration Data

1. **Is this account part of sensitive groups?**
2. **Is this user active? Stale? Password never expires?**
3. **Are there shared credentials across systems?**
4. **Do ACLs reveal excessive permissions or backdoors?**
5. **Is the trust configuration secure (e.g., transitive trusts)?**

🔓 Identifying Vulnerabilities via Enumeration

Weakness	Risk
Over-permissioned users/groups	Privilege escalation
Password policies too weak	Brute-force/login attacks
Misconfigured ACLs (Access Control Lists)	Unauthorized access
Unpatched DCs or legacy systems	Exploitation through known CVEs
Admin shares open (e.g., C, $Admin$)	Lateral movement paths

🕵️‍♀️ Detecting Suspicious AD Enumeration

Indicator	Possible Tool/Method
Large LDAP queries in short time	LDAP brute force
Use of SharpHound or BloodHound	Graph-based privilege attack mapping
Repeated PowerShell AD queries	Recon from compromised workstation
Access to DCs from non-admin hosts	Possible lateral movement
Enumeration during off-hours	Likely unauthorized

🔧 **Tools like Sysmon, Event Logs, and Defender ATP** can help detect this activity.

✅ Summary – Core Skills to Master

- 🧠 Understand AD structure and object relationships.
- 🛠️ Use native tools (PowerShell, `dsquery`) and third-party tools (BloodHound).
- 🔍 Interpret enumeration results to spot:
  - Weak passwords
  - Misconfigurations
  - Excessive permissions
- ⚔️ Think like an attacker to defend like a pro.
